

**AFFIDAVIT IN SUPPORT OF
SEIZURE WARRANT APPLICATION**

I, Bret Curtis, Special Agent, Federal Bureau of Investigation (“FBI”), being duly sworn, declare and state as follows:

INTRODUCTION & PURPOSE OF THE AFFIDAVIT

1. I make this affidavit in support of an application for the issuance of a seizure warrant to seize all Cryptocurrency stored in the OKX¹ Account for User Identification Number (UIN) 617607559549332305 held in the name of BOMETA SIN (**SUBJECT TARGET ACCOUNT**).

2. The **Subject Target Account** is believed to be the proceeds of violations of 18 U.S.C. § 1343 (Wire Fraud) and/or property involved in concealment money laundering in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (Concealment Money Laundering). For the court to authorize seizure of the Target Assets it must find probable cause to believe that: (1) the crimes of Wire Fraud and Concealment Money Laundering were committed; and (2) the Target Assets have a connection to those offenses in the manner specified by the below statutes authorizing forfeiture.

3. For the reasons set forth below, there is probable cause to believe the Target Assets have a connection to Wire Fraud and Concealment Money Laundering and are subject to **civil seizure and forfeiture** under the following forfeiture authorities:

- a. Pursuant to 18 U.S.C. § 981(a)(1)(C) because the Target Assets are property, real or personal, which constitutes or are derived from proceeds traceable to a Wire Fraud. Section 981(a)(1)(C) provides for the civil forfeiture of any property, real or personal, which constitutes or is derived from proceeds from any offense constituting a “specified unlawful activity” as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such offenses. A “specified unlawful activity,” as defined

¹ OKX is cryptocurrency exchange. A cryptocurrency exchange is a platform used to buy and sell virtual currencies and allows users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa.

in Section 1956(c)(7), includes offenses listed in 18 U.S.C. § 1961(1). Section 1961(1) includes Wire Fraud violations.

- b. Pursuant to 18 U.S.C. § 981(a)(1)(A) because the Target Assets were involved in Concealment Money Laundering or are traceable to such property.
- c. Consequently, seizure of the Target Assets for civil forfeiture is authorized by 18 U.S.C. § 981(b).

4. For the reasons set forth below, there is probable cause to believe the Target Assets have a connection to Wire Fraud and Concealment Money Laundering and are subject to **criminal seizure and forfeiture** under the following forfeiture authorities:

- a. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c) because the Target Assets are property, real or personal, which constitutes or are derived from proceeds traceable to Wire Fraud.
- b. Pursuant to 18 U.S.C. § 982(a)(1) because the Target Assets were involved in Concealment Money Laundering or are traceable to such property.
- c. Consequently, seizure of the Target Assets for criminal forfeiture is authorized by 21 U.S.C. § 853(f) and 18 U.S.C. § 982(b).

5. Restraint of the Target Assets under 21 U.S.C. § 853(e) would likely not be sufficient to adequately protect them and preserve their availability for forfeiture and so a seizure warrant pursuant to 21 U.S.C. § 853(f) is necessary. Assets in a cryptocurrency exchange account are fungible and easily transferrable.

6. Although Rule 41(b) of the Federal Rules of Criminal Procedure provides that seizure warrants must be executed in the issuing district, other statutes authorize a magistrate to issue a warrant to seize property outside the district. Under 21 U.S.C. § 853(l), district courts have jurisdiction to authorize a criminal seizure warrant under 21 U.S.C. 853(f) “without regard to the location of any property which may be subject to forfeiture.” The same authority is granted for civil forfeiture seizure warrants under 18 U.S.C. § 981(a) by 18 U.S.C. § 981(b)(3). OKX is in the Seychelles, but they accept U.S. warrants.

BACKGROUND OF AFFIANT

7. I am a Special Agent with the FBI in Salt Lake City, Utah. I have been an FBI Special Agent since February 22, 2004. In my capacity as a Special Agent with the FBI, I have conducted and participated in numerous official investigations into mail and wire fraud, money laundering and other financial and computer crimes as well as drug trafficking crimes. I am a graduate of the FBI Training Academy in Quantico, Virginia and have also attended advanced training classes in the areas of white-collar crime.

8. As an FBI Special Agent, I am familiar with the use of financial accounts by those who operate fraudulent schemes and the types of transactions reflected on financial account records. I am also familiar with the principles of tracing assets into and through financial accounts.

9. The facts set forth in this affidavit are based on my personal observations, my training and experience, my review of documents, interviews with witnesses, and others at FBI assisting with this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested seizure warrant and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

BACKGROUND ON CRYPTOCURRENCY

5. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat (i.e. national currencies like the dollar, euro, yen, etc.) currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other

tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.² Cryptocurrency is not illegal in the United States.

b. Bitcoin³ (“BTC”) is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by “mining.” An individual can “mine” bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as “pseudonymous,” meaning that they are partially anonymous. And while it’s not completely anonymous, bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

² Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

³ Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

c. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or “public key”) and the private address (or “private key”). A public address is represented as a case-sensitive string of letters and numbers, 26–25 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address’ private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

d. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services on hidden services websites. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement’s efforts to track transfers, trades, purchases, and other financial transactions. As of October 31, 2024, one bitcoin is worth approximately \$72,335.05 though the value of bitcoin is generally much more volatile than that of fiat currencies.

e. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible external device (“hardware wallet”), downloaded on a PC or laptop (“desktop wallet”), with an Internet-based cloud storage provider (“online wallet”), as a mobile application on a smartphone or tablet (“mobile wallet”), printed public and private keys (“paper wallet”), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g.

Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code⁴ with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a “recovery seed” (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

f. Bitcoin “exchangers” and “exchanges” are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”) Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.⁵ Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering (“AML”) regulations, “Know Your Customer” (“KYC”) protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions

⁴ A QR code is a matrix barcode that is a machine-readable optical label.

⁵ See “Application of FinCEN’s Regulations to Person Administering, Exchanging, or Using Virtual Currencies,” *available at* <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

g. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

RELEVANT CRIMINAL STATUTES

10. Title 18 U.S.C. § 1343 states:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio or television communication in interstate or foreign commerce, any writings, signs, signals, pictures . . . for the purpose of executing such scheme or artifice.

11. Title 18 U.S.C. § 1956(a)(1)(B)(i) states:

Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

(B) knowing that the transaction is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

FACTS SUPPORTING PROBABLE CAUSE

12. This case involves the receipt of funds traceable to an online investment scam or scheme and the laundering of those proceeds into SUBJECT TARGET ACCOUNT 1 and SUBJECT TARGET ACCOUNT 2.

13. Online Investment Schemes. My investigation has revealed that fraudsters created and coordinated the use of fake online personas, and then used those fake online profiles or personas to engage in online chats, text messaging, and other forms of communication, with an unwitting victim to trick the victims into believing they were involved in real and lucrative investment opportunities. After gaining the victim's trust, the fraudsters then directed the victim to send their own personal funds to the fraudsters. Such frauds are also referred to as confidence scams.

The Fraud Scheme

14. Victim #1, age 63, resides in Herriman, Utah and fell victim to an investment scam in which he believed he was sending money to cryptocurrency wallets to participate in a lucrative online investment involving cryptocurrency.

15. On January 4, 2023, Victim #1 received a text message from a person claiming to be Li Shuyuan ("Li"). After Victim #1 told Li she had the wrong number, Li continued to communicate with Victim #1 via text message. In my experience investigating confidence scams, I have observed some of them begin with a "wrong number" text message like the one Victim #1 received from Li. During the next several months, Li and Victim #1 developed a digital romantic relationship and communicated regularly. Li used multiple phone numbers and WhatsApp numbers to communicate with Victim #1 including a personal number and work number with a Los Angeles, California area code and a WhatsApp number with a Cincinnati, Ohio area code.

16. A Google image search revealed the photographs Li sent to Victim #1 of herself were really of a famous South Korean actress named Park Eun-Ji. Through my training and experience, I have learned it is common for those involved in confidence scams to use the photographs of attractive, sometimes famous individuals from other countries, to entice potential victims into a relationship.

17. On December 12, 2024, I called Park Eun-Ji and spoke to her husband, George Lee. Lee advised that Park Eun-Ji is a celebrity in Korea, and she speaks very little English. Lee confirmed Park Eun-Ji has never communicated with Victim #1 and if Park Eun-Ji's photographs and videos were sent to Victim #1, the person who sent the images did not have Park Eun-Ji's permission to use her image. Lee advised that Park Eun-Ji had nothing to do with the fraud and because her images were used to facilitate fraud Park Eun-Ji should be considered a victim of identity theft.

18. In approximately, February or March of 2023, at Li's encouragement and invitation, Victim #1 and Li began jointly investing in "Ginza," what Victim #1 thought was a legitimate Japan-based e-commerce platform much like Amazon. Li sent Victim #1 an electronic link to the Ginza website at <https://ginza-shop.shop>. Using this link, Victim #1 opened a Ginza account.

19. Li helped Victim #1 open an account on the Ginza website. According to Victim #1, the Ginza website appeared to offer various fulfillment store packages with various product options. Li helped Victim #1 open a fulfillment store on Ginza called Yellowstone Sports & Fashions. Through Li and the Ginza website, Victim #1 believed that he would be able to purchase outdoor sports gear such as fishing poles, boots, and other outdoor products and then sell them through his Gina store.

20. Li told Victim #1 she was introduced to the Ginza platform by an acquaintance identified as Mangzheng Zhu ("Zhu"). Victim #1 and Li were supposed to be paid once the customer received their products. Victim #1 initially invested a couple thousand dollars. Victim #1 sent cryptocurrency to Ginza because he was told that was how Ginza preferred to be paid.

21. Victim #1 stated he was able to monitor his profit in Ginza through an online dashboard. After seeing profits accumulate through his Ginza dashboard, Victim #1 borrowed over \$1,000,000 from friends and family to further invest in Ginza. After investing those funds and seeing significant profits continue in his Ginza dashboard, Victim #1 decided to withdraw \$3.8 million from his Ginza account. However, upon attempting to withdraw the money, Victim #1 was informed by Ginza customer service representatives that he had to pay a Value Added Tax (VAT) of more than \$700,000 before the funds could be released.

22. To help raise the \$700,000, Victim #1 sold his cabin in Island Park, Idaho for \$290,000 in September or October 2024. On October 9, 2024, \$161,752.57 was wired to Victim #1's MACU account from Alliance Title & Escrow LLC. This payment represents proceeds from the sale of Victim #1's cabin. Victim #1 used the proceeds from the sale of his cabin to pay Ginza, so he could withdraw money from his Ginza account. Victim #1 showed documentation of two cryptocurrency transactions he made using the proceeds from the sale of his cabin believing the payments would facilitate Ginza's release of his funds:

Date	Amount Out	Exchange	Notes	Wallet / Account
10/11/24	\$141,691.53	Coinbase	Transfer to Ginza's Wallet	0xdA7Ad625E438860fc4789ff6320a2F62C4E17f89
10/11/24	\$9,001.40	Coinbase	Transfer to Ginza's Wallet	0xdA7Ad625E438860fc4789ff6320a2F62C4E17f89

23. Victim #1 made several payments toward the VAT, but to date, he has not received any payments from his investments in Ginza. After Victim #1 paid Ginza \$700,000, he was told he needed to pay additional taxes and fees because the balance in his account had increased. Victim #1 estimated that he had paid Ginza approximately \$1.4 million in an attempt to withdraw funds. Furthermore, Victim #1 stated that his Ginza fulfillment center has now been shut down and he has been unable to access any of the money in it.

24. Prior to the Ginza center behind closed, Victim #1 communicated with Ginza Customer Service representatives who used email account ginza8888888@gmail.com. After the

Ginza center was closed, Li provided Victim #1 a WhatsApp number (213)646-9312 to communicate with Ginza Customer Service representatives. Victim #1's only communication with Ginza since August 2023 has been through this WhatsApp number.

25. In my training and experience investigating cryptocurrency confidence scams, I have observed perpetrators utilize fake applications that appear to be fully functional and that lull victims through reports that give the appearance of profits like the Ginza dashboard. Such perpetrators also utilize other actors to masquerade as customer service, but which are part of the fraud. Furthermore, the refusal to allow withdrawals of funds until a "tax" or fee is paid follows a similar pattern to other confidence/investment scams I have investigated and suggests that Victim #1's investment through Ginza was fraudulently induced.

26. Another red flag that shows the Ginza website was fraudulent is that it is no longer a registered domain and is not accessible. According to online sources, the website was not operated for a long period having been created on or about May 13, 2023. Agents were able to retrieve a snapshot of the website at <https://web.archive.org/web/20230717024943/https://ginza-shop.shop>. The website listed ginza8888888@gmail.com as its only contact information. The website advertised items for sale ranging from clothing to automobiles. I did identify that there is a legitimate Japanese-based company called the Ginza. Its website can be found at https://www.theginza.com/en_JP/home. The real Ginza website advertises perfume and cosmetic products for sale and listed a phone number of 0120-500824. A note listed next to the phone number advised service was provided in Japanese.

27. Victim #1's Mountain America Credit Union (MACU) account xx2912 records revealed the following wire transfers to different bank accounts to facilitate the purchase of cryptocurrency between October 10, 2024, and November 18, 2024:

Date	Amount Out	Bank	Notes	Wallet / Account
10/10/2024	\$155,000	MACU	Wire to Coinbase Inc.	Cross River Bank 341121519589

10/21/2024	\$50,000	MACU	Wire to Coinbase Inc.	Cross River Bank 341121519589
10/21/2024	\$150,000	MACU	Wire to Coinbase Inc.	Cross River Bank 341121519589
10/23/2024	\$139,000	MACU	Wire to Coinbase Inc.	Cross River Bank 341121519589
10/29/2024	\$194,000	MACU	Wire to Coinbase Inc.	Cross River Bank 341121519589
10/29/2024	\$16,909	MACU	Wire to Coinbase Inc.	Cross River Bank 341121519589
10/30/2024	\$246,000	MACU	Wire to Coinbase Inc.	Cross River Bank 341121519589
10/30/2024	\$240,000	MACU	Wire to Coinbase Inc.	Cross River Bank 341121519589
11/1/2024	\$52,625	MACU	Wire to Community Federal Savings Bank	To 863004068040
11/4/2024	\$300,000	MACU	Wire to Coinbase Inc.	Cross River Bank 341121519589
11/5/2024	\$300,000	MACU	Wire to Coinbase Inc.	Cross River Bank 341121519589
11/8/2024	\$66,000	MACU	Wire to Community Federal Savings Bank	To 863004068040
11/12/2024	\$188,000	MACU	Wire to Coinbase Inc.	Cross River Bank 341121519589
11/13/2024	\$53,468	MACU	Wire to Community Federal Savings Bank	To 863004068040
11/14/2024	\$45,000	MACU	Wire to Community Federal Savings Bank	To 863004068040
	\$2,513,286			

28. Victim #1 provided documentation showing how he transferred cryptocurrency to the following virtual wallets between October 11, 2024, and November 5, 2024, in a failed effort to pay Ginza taxes and fees so they would release money from his account:

Date	Amount Out	Bank	Wallet / Account
10/11/2024	\$141,691.53	Coinbase	0xdA7Ad625E438860fc4789ff6320a2F62C4E17f89
10/11/2024	\$9,001.40	Coinbase	0xdA7Ad625E438860fc4789ff6320a2F62C4E17f89
10/21/2024	\$48,587.52	Coinbase	0xdA7Ad625E438860fc4789ff6320a2F62C4E17f89

10/22/2024	\$50,000	Coinbase	0xdA7Ad625E438860fc4789ff6320a2F62C4E17f89
10/29/2024	\$188,486.86	Coinbase	0x689490ccca7649a5D4801c7aedDad6FE2de87eD
10/30/2024	\$16,899	Coinbase	0x689490ccca7649a5D4801c7aedDad6FE2de87eD
10/30/2024	\$13,418	Coinbase	0xdA7Ad625E438860fc4789ff6320a2F62C4E17f89
10/31/2024	\$239,054.06	Coinbase	0x689490ccca7649a5D4801c7aedDad6FE2de87eD
11/5/2024	\$291,860.94	Coinbase	0x689490ccca7649a5D4801c7aedDad6FE2de87eD
	\$998,999.31		

29. Li told Victim #1 she found investors who were willing to help Victim #1 pay Ginza the taxes and fees he owed so he could withdraw the \$3.8 million from the Ginza account. One of Li's investors was Zhu. Victim #1's MACU account revealed he received \$2,322,294.91 in wire transfers from Zhu's Wells Fargo account xx4486 between October 21, 2024, and November 12, 2024. Li told Victim #1 he could use approximately \$95,000 worth of Zhu's money to pay Ginza, but he had to purchase cryptocurrency for Zhu with the rest of the money she wired to his account. Li told Victim #1 that Zhu's bank would not allow her to buy cryptocurrency. After Zhu wired money to Victim #1's account, Li would provide him with Zhu's wallet to deposit the cryptocurrency into. When investigators told Victim #1 Zhu's wires came from Wells Fargo, which Victim #1 did not realize at the time Zhu sent the funds, Victim #1 was angry because he had purchased cryptocurrency multiple times using his Wells Fargo account and he realized that Li had lied to him about the reason for Zhu needing him to buy cryptocurrency for Zhu.

30. On December 11, 2024, Zhu was interviewed at the San Francisco airport after she arrived on a flight from Beijing, China. Zhu was asked why she wired over \$2,000,000 to Victim #1. Zhu told agents Victim #1 was a sweet lady and a good friend. Victim #1 is a man, and according to Victim #1 he has never met Zhu. Zhu told the agents she was very wealthy, she only sent Victim #1 about \$1,000,000, not \$2,000,000, and it was not a big deal because she had a lot of money. Zhu assured the agents she was not involved in anything illegal, but she refused to answer any more questions without a lawyer present.

31. On December 12, 2024, Li texted Victim #1 and told him the FBI detained Zhu at the airport and asked about money she wired to Victim #1. Li assured Victim #1 that Zhu was: "A

real friend, she is doing some investment, she is also in the United States, the funds she transfers to you are all her personal.”

32. On December 12, 2024, Victim #1 told Li he knew she was not who she said she was. Li admitted she lied about her real identity because, *“I don’t know, if you know the truth, will you still love me?.....Since you know the truth, I don’t think I need to pretend anymore. I will face you with my true self. If you don’t want to accept it, I can quietly leave your life.”*

33. Li’s contact with Victim #1 regarding Zhu’s contact with the FBI suggests that Li and Zhu are in contact with one another. As indicated, Li also told Victim #1 that it was Zhu who introduced Li to Ginza, which the facts above show probable cause to believe was a fraudulent enterprise.

34. On December 16, 2024, I called Zhu and left a voicemail. On the morning of December 17, 2024, Zhu called me back and left a voicemail stating she was told Victim #1 was a public official and the money she wired to his MACU account was supposed to be used to pay taxes. Zhu advised she returned to China and would not be able to take calls.

35. The facts suggest that Victim #1 was being used as a “money mule.” A money mule is someone who transfers or moves illegally acquired money on behalf of someone else. In my training and experience, I know that perpetrators of confidence scams will sometimes try to use their scam not only to defraud the victim of the victim’s money, but also to use the victim as a money mule to launder fraud proceeds obtained from other victims. Money mules add layers of distance between crime victims and criminals, which makes it harder for law enforcement to accurately trace money trails.

Money Mule Activity of Victim #1 Involving Victim #2 and Victim #3

36. In addition to the above conduct involving Zhu and contemporaneous with those circumstances, Victim #1 was also operating as a money mule by collecting money from Victim #2 and Victim #3. While the investigation has not determined if the schemes involving Victim #2 and Victim #3 are part of the same scheme that involved Zhu, the commonalities between the

victimization of Victim #1, Victim #2, and Victim #3, and the transfer of the fraudulently obtained funds provide further context in support of probable cause for seizing the Subject Target Account.

37. Victim #2 is fifty-one years old and lives in Kirklin, Indiana. In June 2024, Victim #2 received a random text message from a person claiming to be Jennifer Pham. Pham told Victim #2 she texted his number on accident, but they started communicating and developed a virtual romantic relationship.

38. Pham encouraged Victim #2 to invest in cryptocurrency. In September 2024, Pham helped Victim #2 open a virtual wallet using Crypto.com. After opening the Crypto.com wallet, Pham helped Victim #2 open a IUEcoin.com account on a fraudulent platform she provided. Pham directed Victim #2 to transfer money from his legitimate Crypto.com wallet to virtual wallets she said were associated to the IUEcoin.com account. The IUEcoin.com wallet showed the deposits and reported large profits. When Victim #2 tried to withdraw money from the IUEcoin.com account he was told he had to pay taxes and fees.

39. On November 1, 2024, Victim #2 wired \$52,624.80 to Victim #1's MACU account because he was told he had to pay an 8% withdrawal fee. Victim #2 was told Victim #1 was a UIEcoin.com business manager. On November 8, 2024, Victim #2 wired \$66,000 to Victim #1's MACU account to pay a fee to convert USDT to U.S. dollars. On November 13, 2024, Victim #2 wired another \$20,000 to Victim #1's MACU account to pay an additional withdrawal fee to remove money from his UIEcoin.com account.

40. Victim #2 was never allowed to withdraw any of the money he invested in the UIEcoin.com account. Victim #2 estimated he lost about \$200,000 to the scam. When asked about the money Victim #2 wired to his account, Victim #1 said he was told the money came from other investors and he was directed to purchase cryptocurrency with the money.

41. Victim #3 is fifty-two years old and lives in Lancaster, Texas. In September or October of 2024, Victim #3 met a person calling herself Jennifer on TikTok. Victim #3 and Jennifer began communicating with each other and started a virtual romantic relationship.

42. Jennifer encouraged Victim #3 to invest in cryptocurrency. She helped Victim #3 open a IUEcoin.com account on a fraudulent platform. She directed Victim #3 to transfer two or three thousand dollars at a time to the fraudulent IUEcoin.com account. The IUEcoin.com platform showed the deposits and reported large profits. When Victim #3 tried to withdraw money from the account he was told he had to pay taxes and fees.

43. On November 27, 2024, Victim #3 wired \$7,904 to Victim #1's MACU account because he was told he had to pay taxes to withdraw money from his UIEcoin.com account. On December 2, 2024, Victim #3 wired \$11,680.20 to Victim #1's MACU account to pay to convert Bitcoin to USDT. On December 3, 2024, Victim #3 wired \$8,955 to Victim #1's MACU account to pay a fee to transfer money from the fraudulent IUEcoin.com account to his legitimate cryptocurrency account.

44. None of the money sent to Victim #1's account by Victim #3 was used for its intended purpose. Victim #3 lost about \$48,539 to the scam. When asked about the money Victim #3 wired to his account, Victim #1 said he was told the money came from other investors and he was directed to purchase cryptocurrency with the money.

Tracing of Funds Zhu Provided to Victim #1 into SUBJECT ACCOUNT

45. An FBI Digital Operations Specialist tracked the movement of the funds Victim #1 paid to Ginza and the funds Victim #1 received from Zhu. Victim #1 sent a series of large transfers to two cryptocurrency addresses including transfers of Victim's 1's funds to Ginza's Wallet and transfers of funds Victim #1 received from Zhu to Zhu's Wallet ("Zhu's Funds"). The funds Victim #1 sent to the Ginza Wallet and to Zhu's Wallet were traced to and commingled in a Consolidation Wallet. From the Consolidation Wallet, Zhu's Funds were sent through multiple cold wallets⁶ and exfiltrated to multiple cryptocurrency exchanges including OKX.

46. In tracing funds, investigators used a last in first out methodology. This method assumes that when dirty funds (last in) are deposited into an account/wallet then those dirty

⁶ A cold wallet is a wallet that is not associated with a specific cryptocurrency exchange.

funds must be spent first (first out) even when subsequent “clean” funds are deposited. Once the entirety of the dirty funds are spent, then the clean funds are used for withdrawals. For example, on October 12, 2024, Victim #1 transferred \$141,751.66 to Ginza’s Wallet (last in). The next transfer out of Ginza’s Wallet was \$150,752.88 on October 12, 2024 (first out). Courts have recognized the use of tracing methods to trace criminal proceeds including in *United States v. Banco Cafetero Panama*, 797 F.2d 1154 (2d Cir. 1986) (approving the use of accounting methods to trace criminal proceeds; government can choose the method).

A. Victim 1’s Initial Transfer of Funds to the Ginza Wallet and to Zhu’s Wallet

47. Victim #1 initially sent six transfers of cryptocurrency from his Coinbase account to two separate wallets, three to each. One address ending in **7f89**⁷ was identified as “Ginza’s Wallet” and another, **87ed**, as “Zhu’s” wallet. On October 12, 2024, 141,751.661973 USDT and on October 21, 2024, 48.614.925881 USDT, was transferred from Victim #1’s Coinbase account to “Ginza’s Wallet” **7f89** (*last in*). On October 12, 2024, 150,752.877 USDT and on October 22, 2024, 48,614,9258 USDT was transferred from “Ginza’s Wallet” to “Ginza Hop 2” (*first out*).

48. Funds from two of the transfers to **7f89** were transferred through wallet **910c** (**Ginza Hop 2**) and then to wallet **c174** (**Consolidation wallet**), and one went directly to **c174**. Funds from two of the transfers associated with **87ed** were moved through **8bd2** (**Zhu Hop 1**) and then to wallet **c174** (**Consolidation Wallet**), and one went directly to **c174**. An illustration of these transfers follows in Exhibit A.⁸

⁷ Wallet addresses are truncated to the last four characters.

⁸ Exhibit A references some terms not previously defined including a smart contract, an unhosted wallet, and a cross-chain swap. A **smart contract** is a computer program that runs automatically when certain conditions are met and is stored on a blockchain or distributed ledger technology. Smart contracts are made up of only computer code, and do not include legal wording or binding contractual obligations. Smart contracts are regularly used to swap cryptocurrencies and conduct automatic transfers. An **unhosted wallet**, also known as a self-custody, a non-custodial wallet, or a cold wallet, gives users complete control over their private keys. This is different from a hosted wallet such as those in a cryptocurrency exchange, where a third party controls the keys. These wallets are used to store cryptocurrency outside the control or management of an exchange. A **cross-chain swap**, often known as an Atomic swap, is a smart contract technology that enables

49. Transaction details of the transfers depicted in Exhibit A include:⁹

Transfers to Ginza's Wallet

Txn Hash	Timestamp	From	To	Asset	Value
0xaa4f27999def0f7d2cc b3962314dfbd537db3ed 022c58183923b038252 5678e7	2024-10-12 00:22:11.000Z	0xa9d1e08c7793af67e9d 92fe308d5697fb81d3e43	0xda7ad625e4388 60fc4789ff6320a2 f62c4e17f89	USDT	141,751.7
0x9f6e4232e9a14faba1 8b296f041d7b0c74d67d 99f665a860d0f36e17ce c31ce4	2024-10-21 19:01:11.000Z	0xa9d1e08c7793af67e9d 92fe308d5697fb81d3e43	0xda7ad625e4388 60fc4789ff6320a2 f62c4e17f89	USDT	48,614.93
0x1b0a66328790176f1b f9d065ecd9ff2b9fbb4ad abd4c68b3f5775a0352d f5efb	2024-10-22 18:06:11.000Z	0xa9d1e08c7793af67e9d 92fe308d5697fb81d3e43	0xda7ad625e4388 60fc4789ff6320a2 f62c4e17f89	USDT	50,033.77

Transfers to Ginza Hop 2 and Consolidation from Ginza's Wallet

Txn Hash	Timestamp	From	To	Asset	Value
0x916a09956d0980106 3311225eff367600b85d b2b70576791f887b08e1 31b2294	2024-10-12 01:01:23.000Z	0xda7ad625e438860fc47 89ff6320a2f62c4e17f89	0xb3bd8d42d22ce 4a2d47021ac7229 28f21282910c	USDT	150,752.9
0xb2d01b384eabd7aeec fd479c4f6ccb37c37afcf 1865517e10d8c011b10 5f2250	2024-10-22 09:47:35.000Z	0xda7ad625e438860fc47 89ff6320a2f62c4e17f89	0xb3bd8d42d22ce 4a2d47021ac7229 28f21282910c	USDT	48,614.93
0xa0c0e78acec4ba8dd3 02887e3273f7a3ec153b 1cd663ae433d857baea3 b1a861	2024-10-22 20:25:11.000Z	0xda7ad625e438860fc47 89ff6320a2f62c4e17f89	0x2d93299b45709 1e10a102e504344 c066246ac174	USDT	50,033.77

Transfers to Consolidation Wallet from Ginza Hop 2

Txn Hash	Timestamp	From	To	Asset	Value
0xa457c4c971c2eca6e5 3919e3dcee84f34cdeab ca718581e0ec8674ba39 f29e99	2024-10-12 01:06:23.000Z	0xb3bd8d42d22ce4a2d47 021ac722928f21282910c	0x2d93299b45709 1e10a102e504344 c066246ac174	USDT	150,000
0x7bd2430031c6f19017 4c41c42f0a8ce1be03d3 ac82be391ad07676866a 65a727	2024-10-22 09:52:47.000Z	0xb3bd8d42d22ce4a2d47 021ac722928f21282910c	0x2d93299b45709 1e10a102e504344 c066246ac174	USDT	50,000

the swap of tokens between two unique blockchains ecosystem. It allows the user to swap tokens directly on another blockchain without any intermediary or central authority.

⁹ The below tables document additional transaction details depicted in Exhibit A and Exhibit B. The tables are color coded to help the reader more easily match the transactions in the tables to the illustrations shown in the Exhibits. For example, in the spreadsheet labeled below as “Transfers to Ginza's Wallet” there are three tables, one highlighted in red, one in orange, and one in green. Those same transactions can be found in Exhibit A depicted with a red line, a green line, and an orange line. The table highlighted in red coincides with the red line in the Exhibit. The same is true with the green table and line and the orange table and line.

Transfers to Zhu's Wallet

Txn Hash	Timestamp	From	To	Asset	Value
0xcd83b4ff6ab4a25b5ac6a4835e5b4705f3ed93a5fc4c7bd5f5a53f1b2207c	2024-10-30 00:49:11.000Z	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x689490ccca7649a5d4801c7aeddad6fed2de87ed	USDT	188,539.5
0xf4a5abf8c03df3180f1913c5836c02e502b6976f8a0d186c7463071804be9069	2024-10-30 21:10:11.000Z	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x689490ccca7649a5d4801c7aeddad6fed2de87ed	USDT	239,107.2
0xe0cd4c394f1464ea4ed27d3565b72ac7665d849720a5088fdb38884f8d51783a	2024-11-05 21:06:11.000Z	0xa9d1e08c7793af67e9d92fe308d5697fb81d3e43	0x689490ccca7649a5d4801c7aeddad6fed2de87ed	USDT	287,675.2

Transfers to Zhu Hop 2 and Consolidation from Zhu's Wallet

Txn Hash	Timestamp	From	To	Asset	Value
0x281889c2cf522a705ff42f8e8fc15e22535e99857813a3d246f1317b15f55c39	2024-10-30 13:37:47.000Z	0x689490ccca7649a5d4801c7aeddad6fed2de87ed	0xb9aaca4f2fc78e52036cb3d6cce2635b788a8bd2	USDT	188,539.5
0x5183fcee7aa54a7bdd278006e49f7c94bd7b9ce26809fafe4d9da10fcf632cd5	2024-10-31 04:52:23.000Z	0x689490ccca7649a5d4801c7aeddad6fed2de87ed	0xb9aaca4f2fc78e52036cb3d6cce2635b788a8bd2	USDT	242,108
0x2da173918e1050f507fb3dac7ef1442200d2820f58eae6ffdaa6e8c0a9e85553	2024-11-05 21:20:59.000Z	0x689490ccca7649a5d4801c7aeddad6fed2de87ed	0x2d93299b457091e10a102e504344c066246ac174	USDT	287,675.2

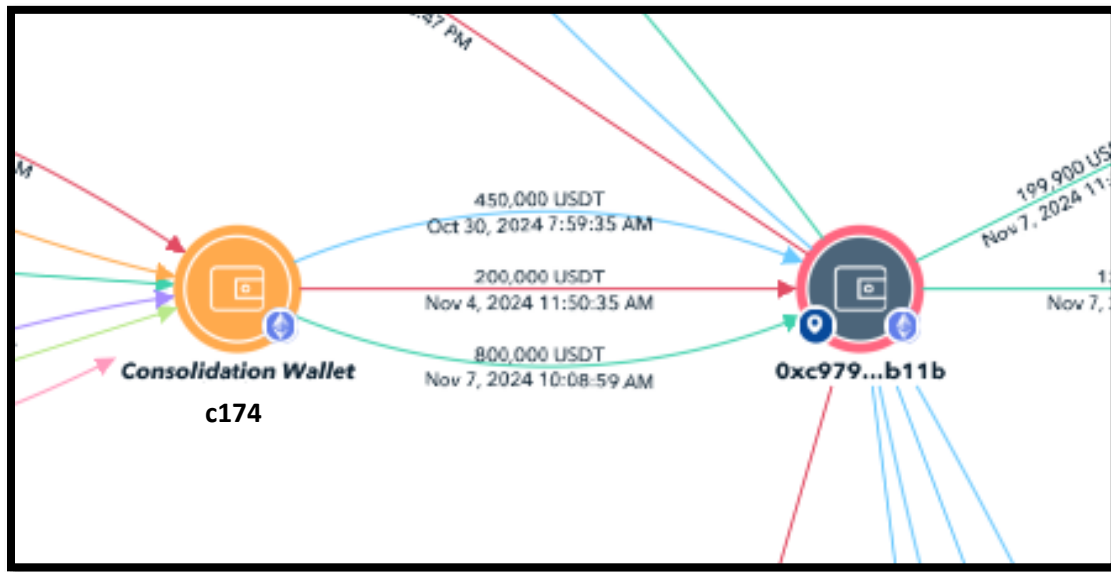
Transfers to Consolidation Wallet from Ginza Hop 2

Txn Hash	Timestamp	From	To	Asset	Value
0x0571fc14777d4ff3fd294f92113873696bde0dddbdc09270028d88eabadd6bf	2024-10-30 13:38:35.000Z	0xb9aaca4f2fc78e52036cb3d6cce2635b788a8bd2	0x2d93299b457091e10a102e504344c066246ac174	USDT	190,000
0x881c8a18bb174d5f9afcd2bb10810e91dc2254fa9a2de6da6a41cbe02f648a	2024-10-31 04:52:59.000Z	0xb9aaca4f2fc78e52036cb3d6cce2635b788a8bd2	0x2d93299b457091e10a102e504344c066246ac174	USDT	240,000

50. From each of the dates Victim #1 transferred USDT from his Coinbase wallet to the Ginza Wallet and to Zhu's wallet, within only about 24 hours roughly the same amounts were transferred to the Ginza Hop 2, Zhu's Hop , and to the Consildation Wallet. That amounts Victim #1 sent to Ginza and Zhu all ended up in the Consolidation Wallet and in such short time frames. This is another indication of Zhu's connection to Ginza.

B. Transfer of Funds from the Consolidation Wallet to b11b

51. Until funds were moved to the Consolidation Wallet (**c174**), they mostly retained their original sums. From the Consolidation Wallet, funds were moved in three transfers and commingled into **b11b** as shown in the following illustration:



52. Transaction details of the three transfers from the Consolidation Wallet to **b11b** include the following:

Transfers from c174 to b11b

Txn Hash	Timestamp	From	To	Asset	Value
0x9424d06640a4acba33f6e23004b066142f7a62ffb712906a45c1fe9939cef9ee	2024-10-30 07:59:35.000Z	0x2d93299b457091e10a102e504344c066246ac c174	0xc97924e9673c299ea0fe7db16648758a64ee b11b	USDT	450,000
0xa9aa19f8b22e1d3b30e1e5e977f0cbda9117315e9e22d976be4a4e668e9e30c1	2024-11-04 11:50:35.000Z	0x2d93299b457091e10a102e504344c066246ac c174	0xc97924e9673c299ea0fe7db16648758a64ee b11b	USDT	200,000
0x67a106fc3c25520d37514a5506831b0832bfc8fbd8d3a6ffca28876786fdf2f3	2024-11-07 10:08:59.000Z	0x2d93299b457091e10a102e504344c066246ac c174	0xc97924e9673c299ea0fe7db16648758a64ee b11b	USDT	800,000

53. Utilizing the last in first out method:

- a. Out of the 450,000 USDT transferred from the Consolidation Wallet to **b11b**, 240,365 USDT is traceable to funds Victim #1 sent to the Ginza Wallet;

- b. Out of the 200,000 USDT transferred from the Consolidation Wallet to **b11b**, all of it is traceable to funds Victim #1 sent to the Ginza Wallet; and
- c. Out of the 800,000 USDT transferred from the Consolidation Wallet to **b11b**, 515,321 USDT is traceable to funds Victim #1 sent to Zhu's Wallet;

C. Tracing of Zhu's Funds to the SUBJECT TARGET ACCOUNT

54. From **b11b**, Zhu's Funds¹⁰ were transferred through varying numbers of cold wallets to a variety of exchanges. After multiple transfers, 199,999 USDT traceable to Zhu's Funds went to deposit address **9cbc** associated with the SUBJECT TARGET ACCOUNT. An illustration of this tracing follows in Exhibit B.¹¹

55. Details for transactions linking Victim #1's funds in **b11b** and traced to address **e339** associated with the SUBJECT TARGET ACCOUNT include:

Txn Hash	Timestamp	From	To	Asset	Value
0xaf488dc7dc0a08d023f35d918ca7c150fdb752ca4c1e6747fe1165d48756c6b7	10/30/2024 9:18	0xc97924e9673c299ea0fe7db16648758a64ee b11b	0xdb8b07cb9ad731045dbb9b1bdb61c745bf0b 0c0f	usdt	50000
0x13b637afb9c7ed9c8b19e28f4442d305216466775838a0b384bd610c08969a80	11/7/2024 10:24	0xc97924e9673c299ea0fe7db16648758a64ee b11b	0xdb8b07cb9ad731045dbb9b1bdb61c745bf0b 0c0f	usdt	199900
0x7a0a870834bae6b0886de0f48ca34186f4ce4fb709193f818c4eac11ed435e0c	11/7/2024 10:46	0xdb8b07cb9ad731045dbb9b1bdb61c745bf0b 0c0f	0xe3192ffdc8b356f00ebf24c14ba6f46e3e 09cbc	usdt	100000
0xd85b694a764724f6646fbd3701c5c73564e865cef10f0c5d8e09b6db49064729	11/7/2024 12:37	0xdb8b07cb9ad731045dbb9b1bdb61c745bf0b 0c0f	0xe3192ffdc8b356f00ebf24c14ba6f46e3e 09cbc	usdt	99999

56. Using the last in, first out methodology, investigators determined that all of the intervening transfers between **b11b** and the SUBJECT TARGET ACCOUNT were traceable to Zhu's Funds making the 100,000 USDT and the 99,999 USDT transferred to the SUBJECT TARGET ACCOUNT on November 7, 2024, entirely traceable to Zhu's Funds. On January 8, 2025, OKX records showed the following cryptocurrency balances in the SUBJECT TARGET ACCOUNT:

¹⁰ Investigators attempted to further trace the funds Victim #1 paid to Ginza, but were unable to trace them to a wallet with a balance that could be seized.

¹¹ One of the transfers from **b11b** went to **64c1**. Wallet **64c1** is marked on the illustration with a "scam" label. This is a label applied by the software utilized by investigators to trace the cryptocurrency.

OKX UID	Account Holder Name	Approximate Balance (USDT equivalent)
617607559549332305	BOMETA SIN	39,745.53

57. Although Zhu has claimed that the funds she gave to Victim #1 was because she was very wealthy and Victim #1 was a sweet lady and a good friend, there is probable cause to believe that this explanation is not genuine and that Zhu's Funds are connected to the same fraud involving Li. In this case, Li told Victim #1 that it was Zhu that introduced her to the Ginza e-commerce platform, a platform that the evidence described above indicates probable cause to believe is fraudulent. Victim #1 made three transfers each to the Ginza Wallet and to Zhu's Wallet. The tracing reveals, and Victim #1 did not know, that the cryptocurrency Victim #1 thought he was sending to Ginza and to Zhu would end up in same wallet. Furthermore, the tracing also reveals a convoluted and circuitous path of transfers within a relatively short time frame between the time Victim #1 initially transferred the funds to the Ginza Wallet and Zhu's Wallet until the cryptocurrency reached the SUBJECT TARGET ACCOUNT.

58. Based on my training and experience, I am aware that individuals engaged in cryptocurrency confidence scams will sometimes move cryptocurrency obtained from the fraud through numerous addresses, cryptocurrency services and exchanges, and accounts to commingle it for the purpose of concealing the nature, source, location, ownership, or control of the fraud proceeds. The transfers in this case appear to fit this paradigm and do not have any indication of legitimate economic character or purpose.

59. In general, a legitimate cryptocurrency transaction should appear much simpler. There is no legitimate reason to move the cryptocurrency to multiple addresses as depicted in Exhibit A and B prior to landing in the OKX account. Through my training and experience I have learned that such movements are indicative of money laundering.

60. Another indication of money laundering present here is the apparent use of funnel account. A funnel account is used by money launderers to funnel fraud proceeds to other accounts.

The Consolidation Wallet was used in this manner as it received both the funds Victim #1 intended to pay Ginza and the funds Victim #1 received from Zhu. Moreover, analysis of the **SUBJECT TARGET ACCOUNT** revealed during the last year, between September 14, 2024, and December 10, 2024, over \$1,000,000 of cryptocurrency was deposited and withdrawn from this account. Through my training and experience, I have learned this volume and the circuitous way Zhu's funds moved prior to reaching the **SUBJECT TARGET ACCOUNT** are indicative of a funnel account.

CONCLUSION

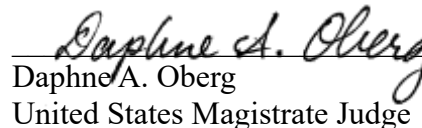
61. Based on the above, there is probable cause to believe that the crimes of Wire Fraud and Money Laundering have occurred and that all cryptocurrency in the **SUBJECT TARGET ACCOUNT** is either proceeds of wire fraud and/or property involved in concealment money laundering. Accordingly, the **SUBJECT TARGET ACCOUNT** is subject to seizure and forfeiture under the authorities described above.

I swear, under penalty of perjury, that the foregoing is true and correct.



Bret Curtis, Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me telephonically this
14th day of January, 2025.



Daphne A. Oberg
United States Magistrate Judge

EXHIBIT A

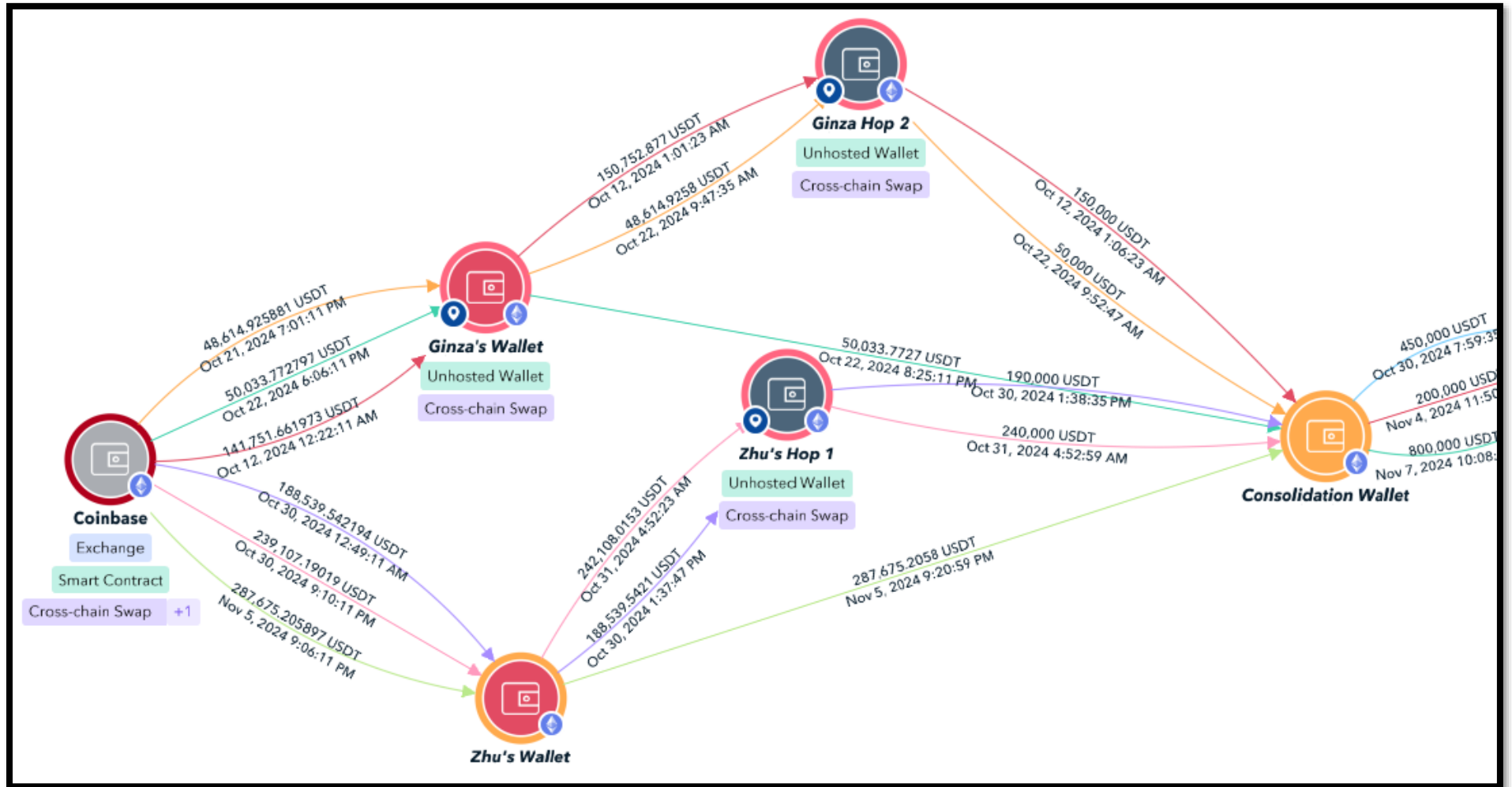


EXHIBIT B

